DATE(S) ISSUED:
01/28/2013

SUBJECT:
Security Bypass Vulnerability in Oracle Java Runtime Environment Could Allow Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in Oracle Java Runtime Environment (JRE) that can lead to remote code execution. The Java Runtime Environment is used to enhance the user experience when visiting websites and is installed on most desktops and servers. This vulnerability may be exploited if a user visits or is redirected to a specifically crafted web page. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the JRE application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely result in denial-of-service conditions.

SYSTEM AFFECTED:
Oracle JRE 1.7.0 Update 10, prior versions may also be affected.

UPDATED SYSTEM AFFECTED:
- ***Oracle JRE 1.7.0 Update 11, prior versions may also be affected.***

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:

A vulnerability has been discovered in Oracle Java Runtime Environment that can lead to remote code execution. In order to exploit this vulnerability, an attacker must first create a web page with a specially crafted applet designed to leverage this issue. When the web page is visited, the attacker supplied code is run in the context of the affected application.

Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the JRE application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely result in denial-of-service conditions.

Please note that there is no patch available from Oracle to mitigate this vulnerability at this time and this vulnerability is being sold in the underground markets.

RECOMMENDATIONS:
The following actions should be taken:

Apply the patch from Oracle, after appropriate testing, as soon as one becomes available.
Consider disabling Java completely on all systems until a patch is available.
Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
Remind users not to visit un-trusted websites or follow links provided by unknown or un trusted sources.
Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.

REFERENCES:

Security Focus:
http://www.securityfocus.com/bid/57563

Full Disclosure:
http://seclists.org/fulldisclosure/2013/Jan/241